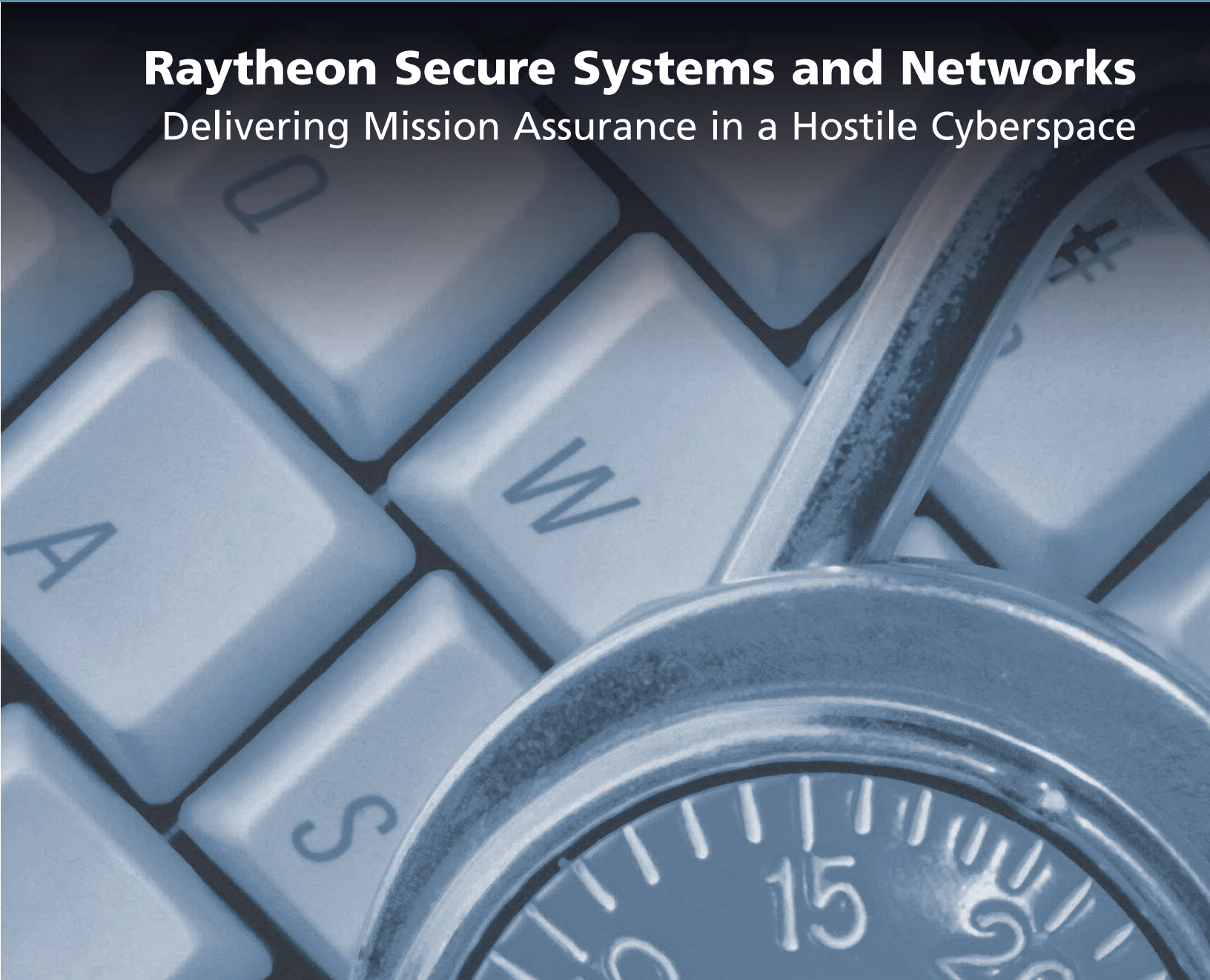


# Technology **Today**

HIGHLIGHTING RAYTHEON'S TECHNOLOGY

2007 Issue 2

## **Raytheon Secure Systems and Networks** Delivering Mission Assurance in a Hostile Cyberspace



**Raytheon**

*Customer Success Is Our Mission*

# Ensuring That Our Systems Can Be Trusted

The systems we build must be trustworthy. That is because the information they provide is used to make decisions on matters of national defense, national security and public safety. Often, these decisions directly concern the safety of the military personnel and public officials of the United States and our allies. Therefore, the end users of our systems — our customers — demand trustworthy information.

All information technology (IT) systems must be certified and accredited in accordance with national policies, federal standards and agency guidelines — regardless of the sensitivity of the information processed on those systems. These standards and guidelines define the certification and accreditation (C&A) processes<sup>1</sup> and information assurance (IA) requirements<sup>2</sup> used to ensure that IT systems can be trusted to protect the confidentiality, availability, integrity and non-repudiation<sup>3</sup> of the information they process.

Proving that our systems are trustworthy is the focus of our customers' C&A processes. The end goal of C&A is to achieve the approval to operate a system by verifying that it provides protection at an acceptable level of residual risk.

The customers' C&A processes do not tell us how to successfully turn a system concept into a secure, certifiable system, and they do not provide a common, unified process for achieving C&A. A common process was first developed by the Information Assurance Technical Framework Forum (IATFF) and termed the Information System Security Engineering (ISSE) process. It provides a standard, dependable way to engineer certifiable

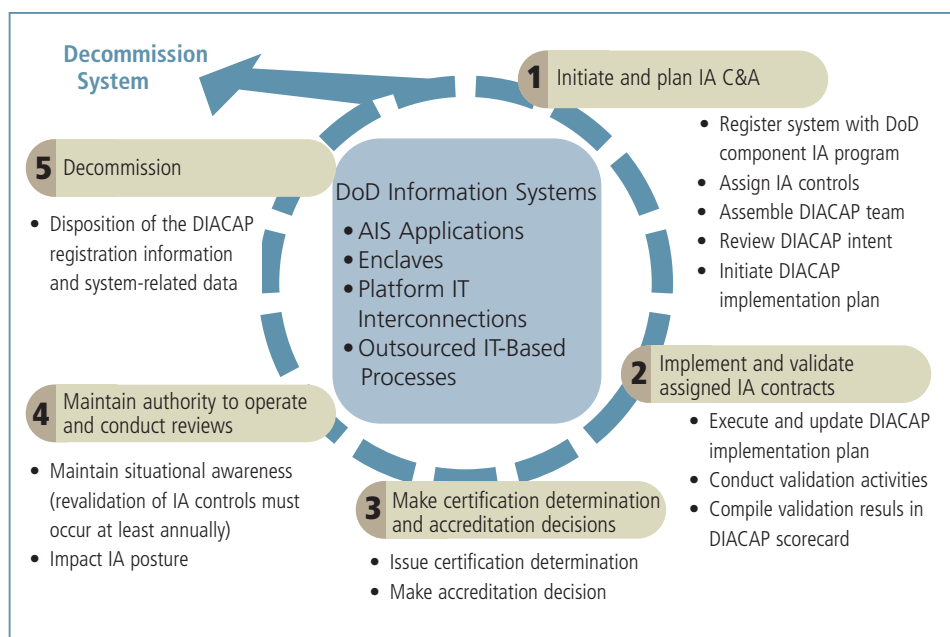


Figure 1. DIACAP Activities Summary

systems and to implement C&A processes. In 2005, Raytheon integrated the ISSE process into its common engineering and product development process.

The C&A processes and Raytheon's ISSE process are integrated into system development from the program startup through deployment. They affect requirements analysis, system design, development, testing and deployment.

## Certification and Accreditation

Our customers' C&A processes are all variations on DoD IA C&A Process Guidance (DIACAP). DIACAP is derived from the DoD Information Technology Security Certification and Accreditation Process (DITSCAP), an earlier standard that it recently superseded. Different customers have tailored versions of the C&A process, but they all work largely as DIACAP does today.

The DIACAP process (see Figure 1) consists of five phases or activities:

1. *Initiate and Plan IA C&A (Definition)* – Define and agree on the system requirement and mission security levels
2. *Implement and Validate Assigned IA Controls (Verification)* – Verify that the

design works and provides the right security

3. *Make Certification Determination and Accreditation Decision (Validation)* – Test the system to ensure it meets all relevant security requirements and can operate at an acceptable level of risk
4. *Maintain Authority to Operate and Conduct Reviews (Post Accreditation)* – Ensure that the system maintains its security configuration and all changes are properly documented
5. *Decommission System*

The C&A process and system development begin with analyzing program objectives, identifying the specific standards and guidelines applicable to the program, and translating these into system level requirements. At this stage, it is important to forge an agreement with the key stakeholders involved in the system development and C&A process.

A continuing partnership must be established at the beginning of the program between the customer program office and

*Continued on page 6*

<sup>1</sup>C&A processes are defined by DITSCAP, DIACAP, DoDIIS C&A Guideline, NIACAP, NISCAP and NIST SP 800-37.

<sup>2</sup>Principal IA requirements documents are DCID 6/3, DoD 8500.2 IA controls and NIST SP 800-53A.

<sup>3</sup>Non-repudiation is a property achieved through cryptographic methods which prevents an individual or entity from denying having performed a particular action related to data (such as mechanisms for non-rejection or authority (origin); for proof of obligation, intent, or commitment; or for proof of ownership).

Continued from page 5

the various stakeholders involved in the C&A process. Early involvement keeps the stakeholder aware of the challenges in securing the system. The typical stakeholders include the program management office, systems developers and integrators, the designated approving authority (DAA), certification authorities and the user organization. This partnership is often referred to as a security accreditation working group (SAWG). It uses a disciplined vetting process to tackle and resolve security issues in order to help achieve accreditation.

During development, the engineering team must design a system to be compliant with applicable security policies and directives. The C&A engineer works closely with other engineers to ensure this compliance, and to ensure that IA operational details are captured in required IA documentation. The working relationship between the C&A engineers and others can make or break the accreditation of the program's cost and schedule.

All hardware and software components are analyzed to determine whether they are IA or IA-enabling products that provide or support security functionality to protect sensitive information. These products include commercial off-the-shelf (COTS) or government off-the-shelf (GOTS) operating systems, firewalls, intrusion detection systems (IDS), and virus protection or encryption devices. During system development, engineers, technicians and managers conduct trade studies to select IA products from a common criteria-evaluated products list of approved IA hardware and software. Products must be evaluated in accordance with specific standards.

Engineers are supported throughout the C&A process by a Web-based knowledge service (KS) provided by the DoD Information Assurance Certification and Accreditation Program (DIACAP). This service provides an authoritative source of C&A information. It contains a library of tools,

diagrams, process maps and documents to support execution of the DIACAP. It offers a workspace for DIACAP users to develop, share and post lessons learned, best practices, and IA events and news. It also provides developers with an online tool for C&A documentation development.

There are several types and levels of accreditation. The system owner will seek formal accreditation for one of the following:

- *Site-based accreditation* – All systems at a single site are consolidated under a single set accreditation
- *Type accreditation* – Multiple instantiations of similar systems with similar configurations, and similar environments at various locations. Each instantiation is under the same Principal Accrediting Authority (PAA).
- *Accreditation of similar systems* – Similar systems are essentially the same based on need to know and access level. The Master Systems Security Plan (SSP)/Systems Security Authorization Agreement (SSAA) may be used for this type of system under the same PAA.

An accreditation boundary that contains all the hardware and software that composes the operational system defines the scope of the system to be accredited.

A system must be accredited to operate at a particular protection level or Mission Assurance category. These levels and categories determine how much security is required based on the sensitivity of the information processed, who has access to the information, and what assurances the system will provide to protect the information. Accordingly, they affect the level of effort required for certification and accreditation.

There are a number of critical success factors in executing the C&A process, including:

- Ensure that program and security managers develop a C&A strategy and get early buy-in from stakeholders

- Make certain that engineering and security management collaborate on the design to ensure that functional and security requirements are nailed down
- Select hardware and software products that meet the assurance levels according to the common criteria
- Keep accreditation boundaries simple so they are clearly understood by the accreditation authority
- Use the security accreditation working group to resolve IA issues; preserve meeting minutes for records of activities discussed and agreed upon during discussions
- Include all C&A activities in the master schedule
- Pay particular attention to CT&E and ST&E activities to ensure all relevant test cases are developed and the results of those test activities validate the security features and functions
- Separate security deliverables from functional deliverables; security deliverables are reviewed and approved by officials with concerns that are separate from functional requirements
- Plan adequate time and resources to fix the findings after the evaluation is complete

### The Raytheon ISSE Process

Raytheon's Information System Security Engineering (ISSE) process is a systems engineering process that addresses the security needs of the system owners and users. It is a generic process designed to meet our diverse customer base. Its purpose is to build trust into the systems we deliver in a reliably repeatable manner.

The steps in the ISSE process mirror those in the systems engineering process we use to define and decompose our customers' requirements, and develop and deliver their systems at the consistently high level of quality they expect. The process is formalized into five process activities. The integration of ISSE steps with each phase of the various C&A processes is shown in Figure 2.

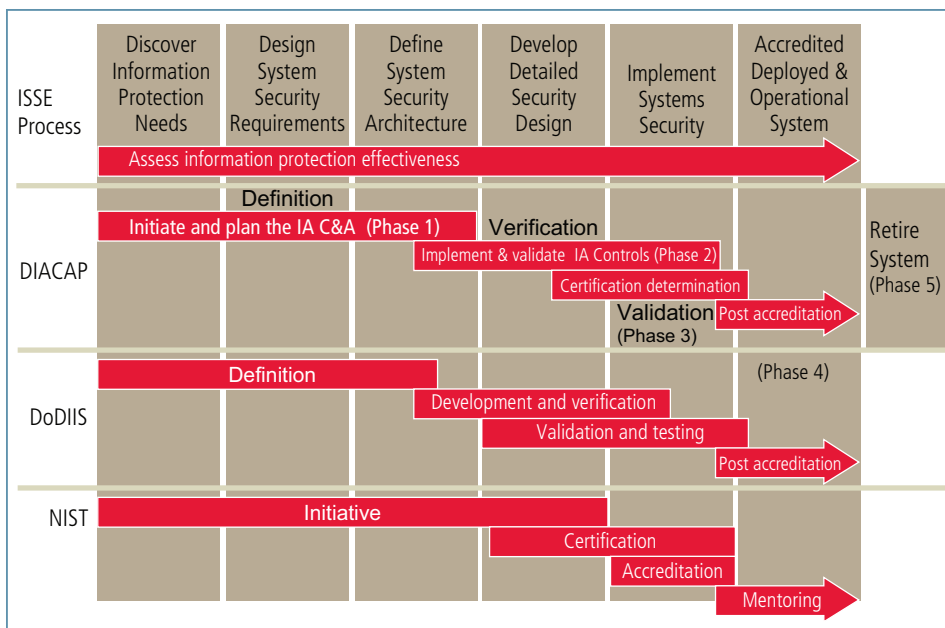


Figure 2. C&A and ISSE processes

### Step 1: Discover customer's information needs

The first activity in the ISSE process is to discover the information needs of the customer. This involves gaining a thorough understanding of the user and the user environment of the system, as well as the data on the system and any data movement into or out of the system (i.e., data flow). Understanding this lets the security engineer develop a sense of the security risks associated with the final deployment of the system. Continued communication with the customer is critical to fully understanding their view of the necessary security of the system. In these discussions, however, both sides should also agree that security is not an absolute — building security into the system must be a risk mitigation activity. The focus of the second activity is the acceptable level of residual security risk that shapes the security requirements.

### Step 2: Define specific system security requirements

Defining specific system security requirements is the goal of the second activity in the ISSE process. Using the customer understanding gleaned in activity one, the security engineer must define system secu-

urity requirements that will ensure the security needs of the customer are met. This also includes ensuring that the system will meet any and all C&A standards levied on the system. Other than being security-specific, these requirements must adhere to the common requirement writing guidelines to which all requirements should adhere. A well-written set of security requirements paves the way for activity three.

### Step 3: Define a system architecture

The third ISSE activity is to use the requirement set defined above and the understanding of the customer's needs to define a system architecture. Here it is critical for the systems engineer and the security engineer to work together to create a system architecture that meets all of the functional and security requirements. Inevitably, this requires compromise on both sides. As with functional requirements, meeting security requirements must be balanced with the customer's cost and schedule needs. On the other hand, the security requirements of the system often create the need for the functional requirements to be met with new approaches.

### Step 4: Develop a detailed security design

Once a system architecture has been defined that meets both sets of requirements, the fourth ISSE process activity can begin: developing a detailed security design. In this activity, security engineers use their knowledge of security products, security functionality of non-security products, the interaction of these products with the custom code being developed for the system, and the underlying hardware and software standards to create a build-to design that meets the security requirements and aligns with the approved architecture.

### Step 5: Implement detailed security design

The final ISSE activity is to implement the detailed security design. It is here that the security engineer interacts with other system implementers to create the system captured in the system architecture above. It is also here that shortcomings of the detailed design or in the system architecture come to light, causing the design and sometimes even the architecture to be tweaked. The security engineer must be a part of all such tweaks to ensure that the security requirements are eventually met. All necessary testing to sell off security requirements and to meet C&A expectations also occurs during activity five.

The ISSE process allows us to assure our customers that we can reliably address their security needs. Addressing our customers' security needs instills trust in the data our systems process and store. It also verifies that the data has not been tampered with and that it will be available when needed to all those (and only those) who need the data. In turn, this increases our customers' trust in us. ●

Robert Batie

robert\_b\_batie@raytheon.com

Jay Coleson

jay\_c\_coleson@raytheon.com

***Do you have a great idea for an article?***

We are always looking for ways to connect with you — our engineering, technology and Mission Assurance professionals. If you have an article or an idea for an article regarding technical achievements, customer solutions, relationships, Mission Assurance, etc., send it along. If your topic aligns with a future issue of *Technology Today* or is appropriate for an online article, we will be happy to consider it and will contact you for more information. Send your article ideas to [techtodayeditor@raytheon.com](mailto:techtodayeditor@raytheon.com). We're waiting to hear from you!

**Raytheon**

*Customer Success Is Our Mission*

Copyright © 2007 Raytheon Company. All rights reserved.  
Approved for public release. Printed in the USA.  
*Customer Success Is Our Mission* is a trademark of Raytheon Company.  
Capability Maturity Model, CMM and CMMI are registered in the U.S.  
Patent and Trademark Office by Carnegie Mellon University.